Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Canceled)

2. (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 wherein an expiration date is not set for the second encryption key.

3. (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 wherein the data input interface also inputs unencrypted data, and the encryption module also encrypts unencrypted data input by the data input interface.

4. (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 further comprising:

a key generator for generating the second encryption key.

5. (Previously Presented) The information processing device of claim 4, further comprising:

volatile memory; and

a memory controller for storing the second encryption key in the volatile memory.

6. (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key using information characteristic to the device itself.

7. (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key when power to the device is turned on.

8. (Previously Presented) The information processing device of claim 4, further comprising:

a media reader capable of being installed with a removable portable storage media storing key generation parameters for reading a key generation parameter stored on the installed portable storage media, wherein the key generator generates the second encryption key using the key generation parameter.

9.   (Previously Presented) The information processing device of claim 4, further comprising:

a device for setting a security level for the information processing device; and

a device for storing the security level of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the security level.

10.   (Previously Presented) The information processing device of claim 4, further comprising:

a device for receiving settings for a region where the device is to be used; and

a device for storing the settings for the region of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the region.

11.   (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 further comprising:

a media reader capable of being installed with a removable portable storage media storing the encryption key, wherein the encryption module reads the second encryption key from the portable storage media installed in the media reader and performs encryption.

12.   (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 equipped with a plurality of the storage devices, and having second encryption keys corresponding to each storage device, wherein the encryption module performs encryption

using the second encryption key corresponding to storage device decided by a data storage destination.

13.   (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 having encryption keys corresponding to each user using the device, wherein the encryption module performs encryption using an encryption key for the user corresponding to the data.

14.   (Canceled)

15.   (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 wherein the deciding device decides to encrypt encrypted data inputted by the data input interface and decrypted by the decryption module.

16.   (Currently Amended) The information processing device of ~~claim 1,~~ claim 19 further comprising:

a printer for decrypting and printing data stored in the storage device.

17.   (Canceled)

18.   (Currently Amended) The information processing device of ~~claim 17,~~ claim 20 further comprising a step of:

storing the second encryption key in the volatile memory.

19.   (New) An information processing device, comprising:

a data input interface for inputting data;

a decryption module for decrypting encrypted data;

an encryption module for encrypting data;

a storage device for storing data; and

a deciding device for deciding whether the input data is encrypted, whether to store the input data and whether to encrypt data decrypted by the decryption module,

-4-

wherein the decryption module decrypts encrypted data input by the data input interface using a decryption key forming a pair with a first encryption key used to encrypt the data,

the encryption module encrypts data decided upon for encryption by the deciding device using a second encryption key different from the first encryption key,

the storage device stores data decided upon for storing by the deciding device, and

the decryption module decrypts encrypted data encrypted by the encryption module and stored in the storage device using the second encryption key.

20.   (New) A method for storing data inputted to an information processing device, comprising:

inputting data;

decrypting encrypted data;

encrypting data;

storing data; and

deciding whether the input data is encrypted, whether to store the input data and whether to encrypt data decrypted by the decryption module,

wherein a decryption module decrypts encrypted data input by a data input interface using a decryption key forming a pair with a first encryption key used to encrypt the data,

an encryption module encrypts data decided upon for encryption by a deciding device using a second encryption key different from the first encryption key,

a storage device stores data decided upon for storing by the deciding device, and

a decryption module decrypts encrypted data encrypted by the encryption module and stored in the storage device using the second encryption key.

21. (New) The information processing device according to claim 19, wherein deciding whether to store the input data is based on a job classification information of the input data.

22. (New) The information processing device according to claim 19, wherein deciding whether to store the input data is based on a time of job processing information of the input data.

23. (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on based on attribute information of the input data.

24. (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a confidentiality information of the input data.

25. (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a storage time of the input data.

26. (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a comparison of at least one of a confidentiality information of the input data or a storage time of the input data to a predetermined threshold value.

27. (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on instruction data provided with the input data.

28.   (New) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on security data that represents a level of security of the storage device.

29.   (New) The information processing device according to claim 19, wherein the deciding device (1) decides based on a job classification information of the input data that the data decrypted by the decryption module is to be printed without the encryption module encrypting the data, and (2) instructs to execute a print process associated with the inputted data after deciding that the data decrypted by the decryption module is to be printed without the encryption module encrypting the data.

30.   (New) The information processing device according to claim 20, further comprising:

deciding based on a job classification information of the inputted data that the data decrypted by the decryption module is to be printed without the encryption module encrypting the data; and

instructing to execute a print process associated with the inputted data after deciding that the data decrypted by the decryption module is to be printed without the encryption module encrypting the data.